UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/614,343	07/08/2003	Gabor Bajko	59643.00228	7843

32294 7590 04/09/2008

SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA, VA 22182-2700

EXAMINER	
FRINK, JOHN MOORE	

ART UNIT	PAPER NUMBER
2142	

MAIL DATE	DELIVERY MODE
04/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/614,343	BAJKO, GABOR	
	Examiner	Art Unit	
	JOHN M. FRINK	2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12,13,22-43,46 and 48-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10, 12-13, 22-43, 46 AND 48-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 12/02/2007 have been fully considered but they are not persuasive.

2. Applicant beings by arguing that "each of the independent claims currently includes limitations analogous to those previously presented in claims 11 and 22. However, Applicants argument is not persuasive. Though the limitations now includes in independent claims, such as claim 1, may be similar to the limitations previously presented in claims 11 and 12, said limitations are not analogous. For example, claim 1 now specifies "determining whether or not the message has been received via the secure interface". Said "secure interface" was not previously claimed in claim 11, rather a "secure means" was claimed. Furthermore, claim 12 did not claim a "secure interface", but rather the specific "Za interface". Thus, Applicant's arguments that new limitations are analogous to previously presented claims 11 and 12 are not persuasive.

3. Next, Applicant presents a similar argument, arguing that "claim 1, analgous to the Za interface of claim 12...". However, as is explained above, the specific "Za interface" of claim 12 is not analogous to the general "secure interface" of claim 1. Thus Applicants argument is again unpersuasive.

4. Applicant next argues that "Arkko fails to disclose or suggest "a receiver configured to receive a message via a secure interface or directly from outside a telecommunications network . . . ". However, Arkko was not cited in the preceeding

office action to show all of said limitations, nor is Arkko cited in the pending office action to show all of said limitations.

5. Applicant next argues that Arkko does not disclose or suggest "using a secure interface as a basis for judging whether or not a message has been through a security check." However, Arkko does teach utilizing a Za interface ([30, 40-41], Fig. 4). Additionally, Arkko shows where a Za interface is utilized for security ([31], showing using a Za interface for negotiating Security Associations (SAs)). The entirety of the claim language of previously presented claim 12, which disclosed said Za interface, was rejected under 35 USC 103, in view of Jennings, Marshall and Arkko. Jennings in view of Marshall teach said "using a secure interface as a basis for judging whether or not a message has been through a security check", as is discussed in more detail in the rejections presented below. Arkko is merely cited to teach said Za interface; furthermore, said Za interface can be utilized for security communications. Applicant's argument thus is not persuasive.

6. Applicant next argues that "Soininen is silent with respect to determining whether a message has been sent through a security check based on whether the message has been received via a secure interface." However, Soininen is not cited to teach all of the above claim language.

7. Applicant next argues on page 25 that "Haukka fails to disclose or suggest, at least, "the security sever being configured to receive a message via a secure interface . . . ". However, Haukka is not citied to teach all of the claim language which Applicant recites on page 25.

8. Applicant's arguments are thus not persuasive. Further details regarding the presently applied art may be found in the pending rejections, presented below.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1–10, 22–29, 31, 33–35, 38-39, 43, 46, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jennings and Peterson (RFC 3325 Internet Draft, http://tools.ietf.org/html/draft-ietf-sip-asserted-identity-00, May 27, 2002), hereafter Jennings, in view of W. Marshall et al. (draft-ietf-sip-privacy-04.txt, February 27, 2002), hereafter Marshall.

11. Regarding claim 1, Jennings shows a receiver configured to receive a message via a secure interface (i.e., from a node that is in its "trust domain", see section 5) or directly from outside a telecommunications network (Section 3, hereafter "(3)");

a determiner configured to determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface; (4, 5, where "secure interface" is represented by a an interface shared with a node it its "trust domain" and thus retains a "P-Asserted-Identity" header).

a forwarder configured to forward the message within the telecommunications network regardless of the result of the determination (4)

Jennings shows when a message *will* not go through a security check, then modifying the message (pg. 6, paragraph 1) but does not show modifying when a message *has not been* through a security check.

Marshall shows a modifier configured to modify the message so as to indicate that the message has not been through a security check if the result of the determination is that the message has not been through a security check (7.5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings with that of Marshall because both disclosures are IETF drafts addressing SIP, and are thus designed to complement each other and be used together.

12. Regarding claim 2, Jennings in view of Marshall further show wherein the receiver is configured to receive a message from outside the telecommunications network (Jennings, 3 and 5).

13. Regarding claim 3, Jennings in view of Marshall further show a modifier configured to modify the message so as to indicate that the message has not been through a security check by adding a parameter to the message that indicates that the message has not been through a security check (Marshall, 7.5).

14. Regarding claim 4, Jennings in view of Marshall further show wherein the receiver is configured to receive a message that includes an identity header and is further configured to add the parameter to the identity header of the message (Jennings, 4 and 5).

15. Regarding claim 5, Jennings in view of Marshall further show wherein the message comprises a session initiation protocol message (Jennings, 5).

16. Regarding claim 6, Jennings in view of Marshall further show wherein the identity header comprises a P-Asserted-Identity (Jennings, 5).

17. Regarding claim 7, Jennings in view of Marshall further show a modifier configured to modify the message so as to indicate that the message has not been through a security check by removing at least part of the identity header,

wherein the receiver is configured to receive a message that includes an identity header (Marshall, 6.1 and 7.5 and Jennings, 4).

18. Regarding claim 8, Jennings in view of Marshall further show a detector configured to detect whether the identity header is of a particular type and if so to remove at least part of the header (Jennings, 4 and 7).

19. Regarding claim 9, Jennings in view of Marshall further show wherein the message comprises a session initiation protocol message (Jennings, 7).

20. Regarding claim 10, Jennings in view of Marshall further show wherein the detector is configured to detect whether the identity header comprises a P-Asserted-Identity type (Jennings, 7).

21. Regarding claim 22, Jennings in view of Marshall further show a system comprising:

a security server; and a network processing element, the security server being configured to (Marshall, 6.1)

receive a message via a secure interface or directly from outside the

system (Jennings, 3 and 5);

determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface (Jennings, 4 and 5 and Marshall, 6.1);

if the result of the determination is that the message has not been through a security check modify the message so as to indicate that the message has not been through a security check (Marshall, 7.5), and

forward the message to the network processing element regardless of the result of the determination (Jennings, 4 and 5 and Marshall, 7.5).

22. Regarding claim 23, Jennings in view of Marshall further show wherein the security server is configured to receive a message from outside the system (Jennings, 3, 5 and 10.2).

23. Regarding claim 24, Jennings in view of Marshall further show wherein the network processing element is configured to:

receive a message forwarded by the security server; and

determine whether the message has been modified so as to indicate that it has not been through a security check, and, if it has been so modified, perform one or more security checks in respect of the message (Jennings, 5 and Marshall 6.1 and 7.5).

24. Regarding claim 25, Jennings in view of Marshall further show a method comprising:

receiving a message via a secure interface or directly from outside a telecommunications network (Jennings, 3 and 5);

determining that the message has not been through a security check by determining that it has not been received via the secure interface (Jennings, 4 and 5);

modifying the message so as to indicate that the message has not been through a security check (Marshall, 7.5); and

forwarding the message within the telecommunications network (Marshall, 6.1 and 7.5).

25. Regarding claim 26, Jennings in view of Marshall further show an apparatus comprising:

a receiver configured to receive a message via a secure interface or directly from outside a telecommunications network (Jennings, 3 and 5);

a determiner configured to determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface (Jennings 4 and 5); and

a forwarder configured to forward the message within the communications network regardless of the result of the determination but, if the result of the determination is that the message has not been through a security check, forward the message in a manner that indicates that the message has not been through a security check (Jennings, 4 and Marshall, 7.5).

26. Regarding claim 27, Jennings in view of Marshall further show an apparatus according to claim 26, wherein the receiver is configured to receive the message from outside the telecommunications network (Jennings, 3 and 5).

27. Regarding claim 28, Jennings in view of Marshall further show an apparatus according to claim 26, wherein the forwarder is configured to forward the message without security, if it is determined that the message has not been through a security check (Marshall, 6.1 and 7.5).

28. Regarding claim 29, Jennings in view of Marshall further show an apparatus according to claim 26, wherein the security server forwarder is configured to forward the message with security, if it is determined that the message has been through a security check (Marshall, 6.1 and 7.5).

29. Regarding claim 31, Jennings in view of Marshall further show wherein the message comprises a session initiation protocol message (Jennings, 5).

30. Regarding claim 33, Jennings in view of Marshall further show a system comprising:

a security server; and a network processing element, the security server being configured to (Marshall, 6.1)

receive a message via a secure interface or directly from outside the system (Jennings, 3 and 5);

determine whether the message has been through a security check by determining whether or not the message has been received via the secure interface (Jennings, 4 and 5 and Marshall 6.1), and

forward the message to the network processing element regardless of the result of the determination, but, if the result of the determination is that the message has not

been through a security check, forward the message in a manner that indicates that the message has not been through a security check (Jennings 4 and 5 and Marshall 7.5).

31. Regarding claim 34, Jennings in view of Marshall further show wherein the security server is configured to receive a message from outside the system (Jennings, 3 and 5).

32. Regarding claim 35, Jennings in view of Marshall further show the system according to claim 33, further comprising:

an internal security system,

wherein the security server is configured to forward the message via the internal security system, if it is determined that the message, has been through a security check (Jennings, 8 and 11 and Marshall, 6.1 and 7.5), and

wherein the security system is configured to not forward the message via the internal security system, if it is determined that the message has not been through a security check (Marshall 6.1 and 7.5).

33. Regarding claim 38, Jennings in view of Marshall further show wherein the message comprises a session initiation protocol message (Jennings, 5).

34. Regarding claim 39, Jennings in view of Marshall further show wherein the security server is configured to determine whether a message has been through a security check by determining whether or not the message has been received via a secure means (Marshall 7.5).

35. Regarding claim 43, Jennings in view of Marshall further show a method comprising;

receiving a message that via a secure interface or directly from outside a telecommunications network (Jennings, 3 and 5);

determining that the message has not been through a security check by determining that the message has not been received via the secure interface (Jennings 4 and 5); and

forwarding the message within the communications network in a manner that indicates that the message has not been through a security check (Marshall 7.5).

36. Regarding claim 46, Jennings in view of Marshall further show an apparatus comprising:

receiving means for receiving a message via a secure interface or directly from outside a telecommunications network (Jennings, 3 and 5);

determining means for determining whether the message has been through a security check by determining whether or not the message has been received via the secure interface (Jennings, 4 and 5);

modifying means for, if the message is determined not to have been through a security check, modifying the message to indicate that it has not been through a security check (Marshall, 7.5); and

forwarding means for forwarding the message within the telecommunications network regardless of whether the message has been through a security check (Jennings, 4).

37. Regarding claim 48, Jennings in view of Marshall further show an apparatus comprising:

receiving means for receiving a message via a secure interface or directly from outside a telecommunications network (Jennings, 3 and 5);

determining means for determining whether the message has been through a security check by determining whether or not the message has been received via the secure interface (Jennings, 4 and 5); and

forwarding means for forwarding the message within the communications network regardless of the result of the determination but, if the result of the determination is that the message has not been through a security check, forwarding the message in a manner that indicates that the message has not been through a security check (Marshall, 7.5).

38. Claims 12, 30, 37, 41, 49, 50, 51, 52, 53, 54 and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jennings in view of Marshall as applied to claim 1, 22, 25, 26, 33, 43, 46 and 48 above, and further in view of Arkko et al. (US 2002/0052200 A1).

Regarding claim 12, Jennings in view of Marshall show claim 1.

Jennings in view of Marshall do not show where the secure interface is a Za interface.

Arkko shows where Za is utilized as a secure interface (Figs. 1 and 4, [30, 40 and 41]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings in view of Marshall with that of Arkko in order to utilize a common security protocol which is intended to be used to enable the

secure exchange of information in systems like Jennings' and Marshall's (Arkko et al., [0040 - 0041]).

39. Regarding claim 30, Jennings in view of Marshall and Arkko further show wherein the security comprises a Zb interface (Figs. 1 and 4, [40 and 41]).

40. Regarding claim 37, Jennings in view of Marshall and Arkko further show wherein the internal security system comprises a Zb interface (Figs. 1 and 4, [40 and 41]).

41. Regarding claim 41, Jennings in view of Marshall and Arkko further show wherein the secure means comprises a Za interface (Figs. 1 and 4, [30, 40 and 41]).

42. Regarding claims 49, 50, 51, 52, 53, 54 and 55 Jennings in view of Marshall and Arkko further show wherein the secure interface is a Za interface (Figs. 1 and 4, [30, 40 and 41]).

43. Claims 13, 32 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jennings in view of Marshall as applied to claims 1, 26 and 33 above, and further in view of Soininen (RFC 3574 Internet Draft, http://tools.ietf.org/html/draft-ietf-v6ops-3gpp-cases-00, September, 2002).

44. Regarding claims 13, 32 and 42, Jennings and in view of Marshall show claims 1, 26, and 33 (Jennings 3, 5, 11.2, Marshall 6.1 and 7.5).

Jennings and in view of Marshall do not show an interrogating call session control function.

Soininen shows where an apparatus comprises and utilized an interrogating call session control function (Section 3.2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings and in view of Marshall and with that of Soininen in order to provide for an SIP system adhering to the 3GPP networking standard (Soininen, Section 3.2).

45. Claims 36 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jennings in view of Marshall as applied to claim 35 above, further in view of Haukka (US 2003/0210678 A1).

46. Regarding claim 36, Jennings in view of Marshall show a system according to claim 35 (Jennings, 8 and 11.2 – 11.5, Marshall 6.1 and 7.5).

Jennings in view of Marshall do not show where the system comprises a UMTS specified security system.

Haukka shows where the system comprises a UMTS specified security system ([0021 - 0023]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the disclosure of Jennings in view of Marshall with that of Haukka in order to provide support for a UMTS network, a common environment utilizing SIP (Haukka, Figs. 1 and 2), which is what Jennings' and Marshall's disclosure was designed to support.

47. Regarding claim 40, Jennings in view of Marshall and Haukka further disclose a system according to claim 39, wherein the secure means comprises a UMTS standard security means (Jennings, Sections 9.1 and 11.2 – 11.4; Haukka, [0021 - 0023]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. Frink whose telephone number is (571) 272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

John Frink

(571) 272-9686

/Andrew Caldwell/
Supervisory Patent Examiner, Art Unit 2142